SEQUENCES OF INTEGERS SATISFYING CONGRUENCE RELATIONS AND PISOT-VIJAYARAGHAVAN NUMBERS

STEPHEN GERIG

(Received 26 October 1966)

1. Introduction

We consider infinite sequences $\{f_n\}_1^\infty$ of positive integers having exponential growth: $f_{n+1}/f_n \to a > 1$, and becoming ultimately periodic modulo each member of a rather sparse infinite set of integers. If sufficient, natural conditions are placed on the growth and periodicities of $\{f_n\}_1^\infty$, we find that a is an algebraic integer having all its algebraic conjugates within or on the unit circle, and f_n has a special representation involving a^n. The result is a kind of dual to the theorem of Pisot (cf. Salem [2], p. 4, Theorem A).

2. Main result

THEOREM. *Let $\{f_n\}_1^\infty$ be a sequence of positive integers, and let $a > 1$ be a real number. Suppose that $|f_{n+1} - af_n| \leqq Qa^{d \log n} = Qn^{d \log a}$, where $Q, d > 0$, and suppose also that $f_1 > QB$, where $B > 0$ is a number, depending only on a and d, to be given explicitly in the proof.*

Assume given an integer $q > 0$, and a set M of p pair-wise relatively prime positive integers. Suppose that the sequence $\{f_n\}_1^\infty$ is ultimately periodic of period $h(m^k)$ modulo m^k, for each $m \in M$ and each positive integer k, periodicity modulo m^k beginning at $n = r(m^k)$.

Assume that p, and the $h(m^k)$ and $r(m^k)$ satisfy

(i) $q^{-1}(p - \sum m^{-q}(m \in M)) > \frac{1}{2}(2d \log a + 1)$,

(ii) $r(m^k) \leqq bm^{qk}$, *and*

(iii) $h(m^k) \leqq cm^{qk}$ *for some fixed positive integers b and c.*

Then a is an algebraic integer all of whose algebraic conjugates lie within or on the unit circle (i.e., *a is a Pisot-Vijayaraghavan or a Salem number* (cf. *Salem* [2])), *and f_n is expressible in the form a^n+terms consisting of n^{th} powers of certain algebraic numbers (all having absolute value $\leqq 1$) with polynomials in n over the rational integers for coefficients.*

Before presenting a proof of the theorem, we state three lemmas.

LEMMA 1 (Hadamard). *Let the $n \times n$ determinant $D = |a_{ij}|$ have real or complex entries. Then $|D|^2 \leqq \prod_{j=1}^n \sum_{i=1}^n |a_{ij}|^2$.*

https://doi.org/10.1017/S1446788700004444 Published online by Cambridge University Press

For a proof see Cassels [1, p. 140].

LEMMA 2 (Kronecker). *The series* $f(z) = \sum_{n=0}^{\infty} a_n z^n$ *represents a rational function if and only if the determinants*

$$D_n = \begin{vmatrix} a_0 & a_1 & \cdots & a_n \\ \vdots & \vdots & \vdots & \vdots \\ a_n & a_{n+1} & \cdots & a_{2n} \end{vmatrix}$$

are zero for all sufficiently large n.

The D_n are called the *Kronecker determinants* of $f(z)$.

LEMMA 3 (Fatou). *If in the series* $f(z) = \sum_{n=0}^{\infty} a_n z^n$ *the* a_n *are rational integers, and if* $f(z)$ *is a rational function, then* $f(z)$ *has the form* $P(z)/Q(z)$, *where* $P(z)$ *and* $Q(z)$ *are polynomials with rational integer coefficients, relatively prime, and* $Q(0) = 1$.

For proofs of Lemmas 2 and 3 see Salem [2, pp. 4—7].

PROOF OF THEOREM. Let $w = d \log a$. Then by the hypotheses of the theorem,

$$f_{n+1} \geqq af_n - Qn^w \geqq a(af_{n-1} - Q(n-1)^w) - Qn^w \geqq \cdots \geqq a_n f_1 - Q \sum_{k=0}^{n-1} a^k (n-k)^w.$$

On the interval $0 \leqq x \leqq n$ define the function $T_n(x) = a^x(n-x)^w$. For $n > d$, consideration of the derivative $T'_n(x)$ shows that $T_n(x)$ increases from n^w at $x = 0$ to a maximum at $x = n-d$, and decreases from there to 0 at $x = n$. For $n > d$, the integral test shows that the series $\sum_{k=0}^{[n-d]-1} a^k(n-k)^w$ is bounded from above by $a^n \Gamma(w+1)(\log a)^{-w-1}$. Simple estimates show that $a^{n-1}(d+1)^{w+1}$ is an upper bound for $\sum_{k=[n-d]}^{n-1} a^k(n-k)^w$. If we set

$$B = \Gamma(w+1)(\log a)^{-w-1} + a^{-1}(d+1)^{w+1}$$

then we conclude that $\sum_{k=0}^{n-1} a^k(n-k)^w \leqq Ba^n$ for $n > d$. Consequently $f_{n+1} \geqq (f_1 - QB)a^n$ for $n > d$. By assumption $f_1 - QB > 0$, and therefore $\{f_n\}_1^\infty$ diverges and also

$$\left| \frac{f_{n+1}}{f_n} - a \right| \leqq \frac{n^w}{f_n} \to 0.$$

It is also easily shown that $f_{n+1} \leqq a^n f_1 + Q \sum_{k=0}^{n-1} a^k(n-k)^w$, which by the estimates made above is less than or equal to $2f_1 a^n$.

If D_n is the n^{th} Kronecker determinant of $\sum_{n=0}^{\infty} f_n z^n$ (where we set $f_0 = 0$), and if $q_j = f_j - af_{j-1}$, then

$$D_n = \begin{vmatrix} f_0 & f_1 & q_2 & \cdots & q_n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f_n & f_{n+1} & q_{n+2} & \cdots & q_{2n} \end{vmatrix}.$$

https://doi.org/10.1017/S1446788700004444 Published online by Cambridge University Press

Lemma 1 applied to this determinant yields

$$D_n^2 \leqq \left(\sum_{j=0}^{n} f_j^2\right)\left(\sum_{j=1}^{n+1} f_j^2\right)\prod_{k=2}^{n}\left(\sum_{j=k}^{n+k} a_j^2\right).$$

We found above that $f_n \leqq 2f_1 a^n$. Thus

$$\left(\sum_{j=0}^{n} f_j^2\right)\left(\sum_{j=1}^{n+1} f_j^2\right) \leqq 4f_1^2\left(\sum_{j=0}^{n} a^{2j}\right)4f_1^2\left(\sum_{j=1}^{n+1} a^{2j}\right) \leqq 16f_1^4(a^2-1)^{-2}a^{4n+6}.$$

By assumption $|q_j| \leqq Q(j-1)^w \leqq Qj^w$ for $j \geqq 2$. Hence for $j \geqq 2$,

$$\sum_{j=k}^{n+k} q_j^2 \leqq Q^2\sum_{j=k}^{n+k} j^{2w} \leqq Q^2(n+1)(n+k)^{2w} \leqq Q^2(n+1)(2n)^{2w}.$$

Thus

$$\prod_{k=2}^{n}\left(\sum_{j=k}^{n+k} q_j^2\right) \leqq Q^{2n}((n+1)(2n)^{2w})^n$$
$$\leqq Q^{2n}\exp\left(n(\log n+\log 2+w\log 2+2w\log n)\right).$$

Therefore

$$D_n^2 \leqq H^2a^{4n}Q^{2n}\exp\left(((w+1)\log 2)n\right)\exp\left((2w+1)n\log n\right),$$

where $H > 0$ is a certain constant. On taking square roots, we make this inequality become

$$(1) \qquad |D_n| \leqq Ha^{2n}Q^n\exp\left((\tfrac{1}{2}(w+1)\log 2)n\right)\exp\left(\tfrac{1}{2}(2w+1)n\log n\right).$$

We now determine a lower bound for the largest integer dividing D_n.

Let $m \in M$, M the set introduced in the statement of the theorem. Let $s = s_m$ be the positive integer for which

$$(b+c)m^{qs} \leqq n < (b+c)m^{q(s+1)}$$

(for the present discussion n is fixed and taken sufficiently large for s_m to exist. $s = s_m$ depends of course on n). Then

$$qs\log m \leqq \log\left(\frac{n}{b+c}\right) < q(s+1)\log m.$$

If $(b+c)m^{q(s-1)} \leqq j \leqq n$, then

$$j-h(m^{s-1}) \geqq j-cm^{(s-1)q} \geqq bm^{q(s-1)},$$

so that the column

$$(2) \qquad \begin{matrix} f(j)-f(j-h(m^{s-1})) \\ \vdots \\ f(j+n)-f(j+n-h(m^{s-1})) \end{matrix}$$

https://doi.org/10.1017/S1446788700004444 Published online by Cambridge University Press

is divisible by m^{s-1} (here $f(i) = f_i$). Therefore if in the determinant D_n we replace each column

$$\begin{matrix} f_j \\ \vdots \\ f_{j+n}, \end{matrix}$$

where $(b+c)m^{(s-1)q} \leqq j \leqq n$, by the column (2), we see that D_n is divisible by

$$\begin{aligned} &\exp\left((s-1)(n-(b+c)m^{(s-1)q}) \log m\right) \\ &= \exp\left((sn-(b+c)(s-1)m^{-q}m^{sq}-n) \log m\right) \\ &\geqq \exp\left((sn-(s-1)m^{-q}n-n) \log m\right) \\ &= \exp\left((ns(1-m^{-q})-n+m^{-q}n) \log m\right) \\ &= \exp\left((ns(1-m^{-q})) \log m\right) e^{An} \\ &\geqq \exp\left[\left\{n(1-m^{-q}) \log\left(\frac{n}{b+c}\right) \frac{1}{q \log m} - 1\right\} \log m\right] e^{An} \\ &= \exp\left(q^{-1}(1-m^{-q})n \log n\right) e^{An}, \end{aligned}$$

where A in each expression is a constant, which may however have different values in different occurrences.

Considering all the $m \in M$, which are all pair-wise relatively prime, we see that D_n is divisible by the integer

$$\prod_{m \in M} \exp\left((s_m-1)(n-(b+c)m^{q(s_m-1)})(\log m)\right) \tag{3}$$

(s_m being the s corresponding to m). Our calculations show that this quantity is bounded from below by

$$\begin{aligned} &\prod_{m \in M} \exp\left(q^{-1}(1-m^{-q})\, n \log n\right) e^{An} \\ &\quad = \exp\left(q^{-1}(p-\textstyle\sum m^{-q}(m \in M))\, n \log n\right) e^{An}. \end{aligned} \tag{4}$$

Comparing this result with the upper bound result for $|D_n|$ given in (1), recalling the hypothesis $q^{-1}(p-\sum_{m \in M} m^{-q}) > \frac{1}{2}(2w+1)$, and observing that $\exp(Bn \log n)$ has a higher order of infinity than $\exp(An)$, we see that there is an $N \geqq 0$ such that for $n \geqq N$, the lower bound (4) for the divisor (3) of D_n is larger than the upper bound given in (1) for $|D_n|$. This implies that $D_n = 0$ for $n \geqq N$.

This result combined with Lemma 2 shows that $\sum_{n=0}^{\infty} f_n z^n$ represents a rational function $R(z)$, and by Lemma 3, $R(z)$ may be written in the form $R(z) = P(z)/Q(z)$, where P/Q is irreducible, P and Q polynomials over the rational integers and $Q(0) = 1$.

Now

$$(1-az)R(z) = \sum_{n=0}^{\infty} f_n z^n - a \sum_{n=0}^{\infty} f_n z^{n+1} = f_0 + \sum_{n=1}^{\infty} (f_n - af_{n-1})z^n.$$

https://doi.org/10.1017/S1446788700004444 Published online by Cambridge University Press

Recalling that $|f_n - af_{n-1}| \leqq Qn^w$ for $n \geqq 2$, we see that the function $F(z) = (1-az)R(z)$ has no poles in the open unit disc. Moreover, $P(z)/Q(z) = (1-az)^{-1}F(z)$, so that a^{-1} is a root of $Q(z)$, and is the only root of $Q(z)$ lying in the open unit disc.

Therefore a is an algebraic number, and even an algebraic integer since $Q(0) = 1$. All of the algebraic conjugates of a, being roots of the polynomial $z^{\deg Q}Q(z^{-1})$ reciprocal to $Q(z)$, lie within or on the unit circle. This means in standard parlance that a is either a Pisot-Vijayaraghavan or a Salem number (cf. Salem [2]).

In addition, it follows from the representation $\sum_{n=0}^{\infty} f_n z^n = (1-az)^{-1}F(z)$ ($F(z)$ a rational function) that f_n is expressible in the form a^n+terms consisting of the n^{th} powers of the poles of $F(z)$, with polynomials in n (with rational integer coefficients) for coefficients. Q.E.D.

3. An example

To show that there are sequences $\{f_n\}_1^{\infty}$ and a number a satisfying the hypotheses of the theorem, let a be a Pisot-Vijayaraghavan number (i.e., a real algebraic integer greater than 1 all of whose algebraic conjugates lie in the open unit disc). If $a_0, \cdots, a_k$ are the algebraic conjugates of $a = a_0$, then for all n sufficiently large, $v_n = \sum_{i=0}^{k} a_i^n$ is the rational integer nearest a^n. If we take $f_n = v_{n+N}$, where N is fixed and sufficiently large, then the inequalities for $|f_{n+1} - af_n|$ and f_1 in the hypotheses of the theorem will be satisfied for some $Q, d > 0$.

Moreover, modulo all sufficiently large m^k, relatively prime to the a_i, the f_n will be ultimately periodic (being a sum of n^{th} powers) of period $\leqq \Phi(L) \leqq \text{norm } L \leqq m^{qk}$, where L is the ideal generated by m^k in the splitting field G of a, Φ is Euler's function for G, and q is a positive integer depending only on G. In addition, all the a_i^n begin being periodic modulo L in time $\Phi(L) \leqq m^{qk}$.

Hence by assigning q the above value, b and c can be found satisfying (ii) and (iii), and by including enough pair-wise relatively prime m, relatively prime to the a_i, in M, (i) can be fulfilled as well.

References

[1] J. W. S. Cassels, *An introduction to Diophantine approximation* (Cambridge Tracts in Mathematics and Mathematical Physics, 45, Cambridge University Press, Cambridge, 1957).

[2] Raphael Salem, *Algebraic numbers and Fourier analysis* (Heath, Boston, 1963).

The University of Western Australia